United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, D.C. 20240

U.S. Department of the Interior
1849 • 1999

October 29, 1998

MEMORANDUM

To: Bureau/Office Management Control Coordinators

From: Claude Christensen, Acting Chief */original signed by*
Program Planning, Review and Standards Division
Office of Information Resources Management

Subject: FY 1999 IRM Management Control Reviews Guidance

This memorandum transmits the Department's FY 1999 IRM management control review requirements. Our guidance this year encompasses two mandatory Departmentwide functional review (DFR) components: **general support systems; and major applications.** It also addresses additional, optional, IRM review components such as **telecommunications systems and non-major applications**. Revised OMB Circular A-130, dated February 8, 1996, mandates a 3-year review cycle for general support systems and major applications.

General Support Systems Reviews

In accordance with OMB guidance, bureaus and offices must conduct management control reviews of all general support systems on a 3-year cycle. The focus of the review should be on the security controls, as outlined in OMB Circular A-130. The scope of the review should be commensurate with the acceptable level of risk for the system. OMB defines a general support system as "an interconnected set of information resources under the same direct management control which shares common functionality." For example, a general support system can be a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. Normally, the purpose of a general support system is to provide processing or communications support. General support system reviews should be performed using a combination of the following Office of Information Resources Management's (OIRM) Management Control Review Guidelines: "Minicomputer Installation Management Control Evaluation Guideline," dated March 1994; the "Mainframe Installation Management Control Evaluation Guideline," dated November 1994; the "Telecommunications Systems Management Control Evaluation Guideline," dated November 12, 1992, and the latest draft chapters for reviewing local and wide-area networks. **Please submit a list of the general support systems you plan to review in FY 1999 to OIRM by November 30, 1998.**

Major Applications Reviews

In accordance with OMB guidance, bureaus and offices must conduct management control reviews of all major applications on a 3-year cycle. The focus of the review should be on the security controls, as outlined in OMB Circular A-130. The scope of the review should be commensurate with the acceptable level of risk for the application. OMB defines a major application as “an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.” Major application reviews should be performed in accordance with OIRM's "Automated Information System (AIS) Management Control Review Guidelines," dated March 1994. Bureaus and offices are also encouraged to use Federal Information Processing Standards Publication (FIPS PUB) 102, "Guideline for Computer Security Certification and Accreditation;" NBS Special Publication 500-109, “Overview of Computer Security Certification and Accreditation;” NIST Special Publication 800-12, “An Introduction to Computer Security: The NIST Handbook;” or the Department of Commerce's NISTIR 4451, "Methodology for Certifying Sensitive Computer Applications," as basic reference documents for certifying/recertifying major applications. Bureaus and offices are requested to forward to OIRM copies of the documentation certifying/recertifying major applications. **Please submit a list of the names of the major applications you plan to review in FY 1999 to OIRM by November 30, 1998**.

Optional IRM Review Components

Non-major Applications: Bureaus and offices are encouraged to perform reviews of non-major applications in conjunction with the review of the functional component supported by the application. These reviews should be performed using OIRM's "Automated Information System (AIS) Management Control Review Guidelines," dated March 1994.

Telecommunications Systems: Telecommunications systems reviews can be performed as part of a general support system review or as an independent review. Telecommunications system reviews should be scheduled based on your priority risk rating for that component. For example, telecommunications components with a high priority risk rating should be reviewed every 3 years; medium priority ratings every 4 years; and low priority ratings may be postponed and/or canceled. Telecommunications reviews should be performed in accordance with OIRM's "Telecommunications Systems Management Control Evaluation Guideline," dated November 12, 1992, and the latest draft chapters for reviewing local and wide-area networks. Bureaus and offices are also encouraged to use Departmental Manual, Part 377, "Telecommunications," as a basic reference document when conducting telecommunications reviews. **Please submit a list of the telecommunications systems you plan to review in FY 1999 to OIRM by November 30, 1998.**

IRM Criteria for Determining a Potential Material Weakness

Bureaus and offices should consider identifying a potential material weakness if there is no assignment of security responsibility, no security plan, or no authorization to process for a general support system and/or a major application. Also, the lack of fully documented and tested Contingency Plan usually constitutes a material weakness. The Department will assess the potential for material weaknesses on a case-by-case basis.

Review Reporting Requirements

The results of the general support systems, major applications and telecommunications systems reviews should be summarized in a report using the procedures prescribed in OIRM's review guidelines and PFM's "Management Control Handbook" dated March 2, 1992. Excerpts from the OIRM guidelines, providing instructions for the written report, are attached. The report(s) must be approved by the head of the bureau and sent directly to OIRM. **The original report(s) should be submitted to OIRM no later than July 15, 1999**, with copies furnished to your Assistant Secretary, the Office of Financial Management (PFM), and the Office of Inspector General.

Questions or comments concerning the guidance for general support systems, and major application reviews may be directed to Sharon Michel at (202) 208-3321. Questions or comments concerning the guidance for telecommunications systems reviews may be directed to Jim Dolezal at (202) 208-5002.

cc: Bureau IRM Coordinators
Bureau IRM Management Control Coordinators
Bureau IT Security Managers
Bureau Telecommunications Managers
Office of Financial Management

Attachment

(Attachment - Excerpt from OIRM Mainframe Computer Installation Management Control Review Guidelines)

V. FUNCTIONAL CONTROL EVALUATION REPORTING PROCEDURE

The results of the control evaluation of the mainframe computer installation should be reported in accordance with established Office of Financial Management (PFM) procedures. After approval by the bureau or office head and the appropriate Assistant Secretary, **the original report should be submitted to the Office of Information Resources Management**, with copies furnished to PFM and the Office of Inspector General. The report should be in the form of a memorandum and have as attachments Exhibits 1 and 3 of this section, as appropriate. The cover memorandum should contain the following information:

- A general description of the mainframe computer installation environment detailing the name and location of the center; the number and type of personnel on board; the vendor, model, and amount of each type of equipment; the type of system software used; the number of applications programs processed at the installation; and **identification of all sensitive information systems supported.**

- A statement to the effect that either:

  "All prescribed controls or alternate controls are in place and effective, as indicated in Exhibit I, and no known control weaknesses exist at the mainframe computer installation." or

  "The lack of prescribed controls or alternate controls or the failure of these controls to be effective, as indicated in Exhibit I, has resulted in the control weaknesses identified in Exhibit 3."

- A list of the functional elements and control techniques excluded from the evaluation and the reasons they were excluded (e.g., "This installation does not charge its users, therefore, Section II.E User Billing and Chargeback Controls is not applicable.").

- A list of any alternate functional elements or control techniques and the controls they replaced.

- A brief summary (one or two paragraphs) of the tests that were conducted to validate the functional elements; which functional elements received special in-depth testing; and the reason for the special tests (e.g., ongoing problems known to installation or bureau management, problems revealed in an OIG report).

- The organizational component(s) that conducted the control evaluation.

The "General Controls Profile" form at Exhibit 1 should be completed and submitted as an attachment to the control evaluation report. Reviewers should provide either a "yes," "no," or N/A (not applicable) response to the first four questions on the form for every control category. A "yes" response should be provided if the statement is always true (i.e., all applicable controls are 100% adequate). A "no" response should be indicated if the statement is not 100% true (i.e., some of the applicable control techniques are not in place). "N/A" should be indicated only for the third and fourth questions if alternate controls do not apply. **Reviewers should use the chart at Exhibit 2 "Worksheet for Assessing the level of Potential Material Weakness" to determine their response to the fifth question on the form.**

The process of determining whether the control objectives of each functional area have been achieved is a subjective process. If all the control techniques are in place and effective, there is, of course, a low potential for material weakness and no control weaknesses will be reported. **Any determinations beyond that will be dependent upon which specific control techniques have not been complied with and the general control environment governing the development effort**. In determining the materiality of an identified weakness, reviewers should consider the criteria contained in 340 DM 2.7F.

The "Control Evaluation Report" at Exhibit 3 is the same form required in other types of control evaluation reports and should only be included as an attachment when control weaknesses are identified in the review. **Each control category identified as having a medium or high level of potential for material weakness must have the specific weakness listed on this form**. The weaknesses reported should be keyed to the control category and the control technique. For example, the failure to maintain an inventory of all systems software and applications software, which is control technique 1 under functional control category "1A" of the General Management Controls would be identified as "I.I.A.1" in Exhibit 3.

Each weakness must be identified by type (i.e., as a weakness either in system design or in compliance with established controls; and as either a material or nonmaterial weakness). For example, failure in having a fully documented and tested Contingency Plan for a mainframe computer that supports one or more major information system applications would constitute a material weakness and would not be in compliance with established controls. If a potential material weakness is identified, an "X" should be placed in the "TYPE" column under the capital "M" heading. The specific actions that will be taken to correct the weaknesses along with the proposed dates for making the corrections must also be reported on the form.

Documentation for all aspects of the control evaluation should be retained in bureau files for potential review by PIR, the OIG, and/or the General Accounting Office. PIR will randomly sample bureau reports to determine the extent of testing, so bureaus should be prepared to submit their control evaluation documentation for PIR review.

Reviewers may find it expedient to use a spreadsheet, like the Departmental guidelines, for documenting their reviews. Use of a spreadsheet will help minimize the amount of documentation required and assist in performing the review. The fully completed spreadsheet, along with the test plan, can then serve as the permanent record of the minicomputer's control evaluation.

GENERAL CONTROLS PROFILE

Exhibit 1

Bureau of Office Name

Minicomputer Installation Name

	Functional Controls	Are the controls in place?	Are the controls adequate?	Are alternate controls in place?	Are alternate controls adequate?	Potential* for material weakness?
I.	General Management					
	A. Resource Planning					
	B. Policy, Standards, and Procedures					
	C. Organization					
II.	Hardware Management					
	A. Scheduling, Data Flow, & Performance					
	B. Equipment Operation					
	C. Media Storage and Retrieval					
	D. Network Management					
III.	System Software Controls					
	A. Operating System					
	B. System Utility					
	C. File Maintenance Software					
	D. Data Communications Software					
	E. System Software Change					
	F. User Billing/Charge-Back					
IV.	Security Controls					
	A. Administrative					
	B. Physical					
	C. Technical					
	D. Contingency Plan					

*Refer to Exhibit 2 when determining the potential for material weakness.

Exhibit 2

WORKSHEET FOR ASSESSING THE LEVEL OF POTENTIAL MATERIAL WEAKNESSES

Two primary criteria should be used to determine the degree of potential material weakness with the mainframe computer installation: Is a control in place and is it adequate? The following chart is strictly a sample of the possible levels that could be assigned to specific functional controls.

			Is some	Is the	
	Is the	Is the	alternate	alternate	Potential
	control	control	control	control	for material
Functional Control	in place?	adequate?	in place?	adequate?	weakness?
I.A Resource Planning	Yes	Yes	No	---	Low
I.C Organizational	No	---	Yes	Yes	Medium
II.A Scheduling, Data Flow, and Perf.	Yes	No	Yes	Yes	Medium
II.C Network Management	Yes	No	No	---	High
III.A Operating System	No	---	No	---	High
IV.A Administrative Security	Yes	Yes	Yes	Yes	High
IV.D Contingency Plan	No	No	No	___	High

Exhibit 3

CONTROL EVALUATION REPORT

BUREAU/OFFICE:

COMPONENT:

RESPONSIBLE OFFICIAL:

DATE:

NO.	IDENTIFIED CONTROL WEAKNESSES	TYPE*				PLANNED CORRECTIVE ACTION	DATE SCHL'D
		S	C	M	m		

*Indicate the type of weakness by checking the appropriate column.